UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF NEW YORK

CAPITAL DISTRICT PHYSICIANS' HEALTH PLAN, INC.
6 Wellness Way
Latham, NY 12110

and

CDPHP UNIVERSAL BENEFITS, INC.
6 Wellness Way
Latham, NY 12110

Plaintiffs,

v.

CHANGE HEALTHCARE TECHNOLOGIES LLC
5995 Windward Parkway
Alpharetta, GA 30005

and

CHANGE HEALTHCARE SOLUTIONS LLC
424 Church Street, Suite 1400
Nashville, TN 37219

and

CHANGE HEALTHCARE RESOURCES LLC
424 Church Street, Suite 1400
Nashville, TN 37219

Defendants.

Civil Action No.: 1:25-cv-233 (AMN/TWD)

COMPLAINT

Plaintiffs, Capital District Physicians' Health Plan, Inc. and CDPHP Universal Benefits, Inc., by and through undersigned counsel, hereby demand judgment against Defendants, Change Healthcare Technologies, LLC, Change Healthcare Solutions, LLC, and Change Healthcare Resources, LLC, and in support thereof, allege the following:

PARTIES

1. Plaintiffs are not-for-profit organizations organized and existing under the laws of the State of New York, with their principal places of business located at the address above.

2. Defendant, Change Healthcare Technologies LLC, is a limited liability company organized and existing under the laws of the state of Delaware, with its principal place of business located at the address above. Defendant is a citizen of Delaware and Tennessee.[1]

3. Defendant, Change Healthcare Solutions LLC, is a limited liability company organized and existing under the laws of the state of Delaware, with its principal place of business located at the address above. Defendant is a citizen of Delaware and Tennessee.[2]

4. Defendant, Change Healthcare Resources LLC, is a limited liability company organized and existing under the laws of the state of Delaware, with its principal place of business located at the address above. Defendant is a citizen of Delaware and Tennessee.[3]

JURISDICTION AND VENUE

5. Jurisdiction is based on 28 U.S.C. §1332(a)(1) as this action involves a controversy between parties of different states. Moreover, the amount in controversy exceeds the jurisdictional threshold of this Court (exclusive of interest and costs).

---

[1] The sole member of Change Healthcare Technologies LLC is the Delaware limited liability corporation, Change Healthcare Holdings LLC. The sole member of such LLC is the Delaware limited liability corporation, Change Healthcare Intermediate Holdings, LLC. The sole member of such LLC is the Delaware limited liability corporation, Change Healthcare LLC. The members of such LLC are Delaware limited liability corporations, PF2 PST Services LLC and PF2 IP LLC, and Delaware corporation, Change Healthcare Inc. The sole members of PF2 PST Services LLC and PF2 IP LLC are Delaware corporation, Change Healthcare Inc. Change Healthcare Inc.'s principal place of business is in Tennessee.

[2] The sole member of Change Healthcare Solutions, LLC is Change Healthcare Operations, LLC. The sole member of Change Healthcare Operations, LLC is Change Healthcare Holdings, Inc. Change Healthcare Holdings, Inc. is a Delaware corporation with its principal place of business in Tennessee.

[3] The sole member of Change Healthcare Resources LLC is Change Healthcare Resources Holdings, Inc., a Delaware corporation with its principal place of business in Tennessee.

6. Venue is proper in this district based on 28 U.S.C. §1391(a) in that the events giving rise to this claim occurred within this district.

FACTS

7. Plaintiffs provide health insurance and related services to their customers.

8. Pursuant to various contracts and related terms and conditions with Plaintiffs (collectively the "Agreements"), Defendants agreed to provide a number of different services to Plaintiffs, including but not limited:

a. Claims Processing: Defendants' clearinghouse electronically transmitted insurance claims from medical care providers to Plaintiffs and payment from Plaintiffs to such providers for their services;

b. Check Printing: Defendants handled the printing of Plaintiffs' checks for payment to certain medical care providers for their services and members for reimbursement of applicable claims;

c. Explanation of Payment ("EOP") Printing: Defendants printed EOPs for Plaintiff, required by regulatory bodies to accompany payments made to medical care providers for their services;

d. Risk Adjustment: Defendants' application provided commercial risk adjustment services required by the Affordable Care Act;

e. Edge Server: Defendants' application provided certain claim and enrollment data on Plaintiffs' behalf to the Department of Health and Human Services pursuant to applicable regulations.

9. On or about February 21, 2024, Defendants experienced an entirely foreseeable and preventable ransomware incident.

10. "Ransomware" is a form of malicious software or malware designed to encrypt files on computer devices, rendering any files and the systems that rely on them unusable. After deploying their malware to cripple vulnerable computer systems, malicious "threat actors" then demand ransom in exchange for decryption.

11. Defendants were a prime target for ransomware attacks because they have significant resources to pay ransoms and because the information they and/or their affiliates collect and store is valuable on black markets.

12. Defendants and/or their affiliates possessed highly sensitive data about millions of individuals as a result of the services they provided, not only to Plaintiffs, but to large portions of the entire healthcare industry.

13. According to testimony given before Congress by those affiliated with Defendants, the ransomware incident occurred after the username and password of a low-level, customer support employee for their access to Defendants' Citrix portal was posted in a Telegram group chat that advertises the sale of stolen credentials.

14. While the account was a basic, user-level account with access only to specific applications, the compromised account had the authority to create accounts with administrative privileges.

15. The compromised account was also not protected by multi-factor authentication.

16. Using the compromised credentials, the threat actors were thereafter able to infiltrate large swaths of Defendants' computer systems and servers wholly unnoticed by Defendants.

17. The threat actors exfiltrated terabytes of data belonging to millions of individuals and demanded Defendants and/or its affiliates pay a large ransom.

18. On February 21, 2024, upon discovering the ransomware, Defendants and/or their affiliates intentionally made the applications and services it provided to its customers inoperable. Defendants also announced the ransomware incident publicly.

19. Though Defendants have since restored all services to Plaintiffs, as a result of the incident, Defendants suddenly and without warning stopped providing Plaintiffs with their contracted-for services for varying periods of time.

20. As a result of the sudden loss of Defendant' services, Plaintiffs were forced to retain alternate vendors or take the services in-house at their own increased expense in order to continue to operate at or around the same capacity as before the incident.

21. As a result of the sudden loss of Defendants' services, Plaintiffs were also required to pay for additional internal labor in order to facilitate the retention of these new vendors and the undertaking of the services in-house. Plaintiffs were also required to expend monies for resources necessary to carry out the services in-house, like printers, check print stock, and ink.

22. In total, between the cost for the new vendors, the additional labor of their employees, and the resources expended, Plaintiffs suffered damages in excess of $800,000.00 as a result of the incident.

COUNT I – BREACH OF CONTRACT

23. Plaintiff incorporates the preceding paragraphs by reference herein.

24. In the Agreements, Defendants promised to provide the contracted-for services, including the license to various software and applications necessary for such services, pursuant to the terms of the Agreements.

25. In breach of their promises to provide such services and the various express warranties related to the provision of the services, Defendants intentionally stopped providing such services, or were compelled to stop providing such services as a result of their own gross negligence, recklessness, and willful misconduct in the securing of their own computer systems.

26. Defendants further breached the Agreements by failing to comply with the provisions of the Agreement related to the Suspension or Termination of the services before suspending and/or terminating the services it provided Plaintiffs.

27. Defendants also breached the Agreements by failing to provide contracted-for remedies related to its failure to perform their services.

28. Moreover, in breach of the Agreements, Defendants failed to maintain adequate safeguards to ensure the security, confidentiality, and integrity of Plaintiffs' use of Defendants' services. These required safeguards were repeated throughout various components of the Agreements, including standards set forth in Business Associate Agreements and Security Standards incorporated into the Agreements, and other areas.

29. Defendant further breached promises in the Agreements to have a viable disaster recovery and business continuity plan.

30. As a direct and proximate cause of Defendants' breaches of the Agreements, Plaintiffs suffered the damages described above.

WHEREFORE, Plaintiffs respectfully request judgment against Defendants in an amount in excess of $800,000.00 plus costs incident to this suit, and attorney fees, and for such other relief as this Honorable Court shall deem appropriate under the circumstances.

de LUCA LEVINE LLC

BY: 

Kenneth T. Levine, Esq.
Andrew G. Hunt, Esq.
301 E. Germantown Pike, 3rd Floor,
East Norriton, PA 19401
215-383-0081
215-383-0082 (fax)
Klevine@delucalevine.com
ahunt@delucalevine.com
ATTORNEYS FOR PLAINTIFF

Dated: February 21, 2025